Additional drafting proposals by the Netherlands regarding the interplay between NIS and CSA / GDPR

(2 June 2021)

Art.	Commission proposal	Drafting proposal	Motivation
Rec 26 [GDPR]	Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this directive.	Given the importance of international cooperation on cybersecurity CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this directive. **In addition, CSIRTs should be able to exchange information, including personal data, with national CERTs and CSIRTs of third countries for the purpose of their tasks. Such disclosure or exchange may constitute important reasons of public interest, especially in the event of a significant cyber threat or any incident having significant effect on the provision of service.**	• Cybersecurity incidents are not confined by borders. The exchange of information as described in recital 69 is therefore necessary not only within the Union, but also by CSIRTs with other CERTs and CSIRTs in the world. • More specifically, international cooperation might not be sufficiently effective in view of the objectives of this Directive if it is not possible to exchange data as referred to in recital 69 with third countries. • For this reason, it is important to identify the tasks of CSIRTs for the purposes of ensuring network and information security of essential or important entities, as referred to in Annex I and II, as public interest, as referred to in article 49 (1)(d) and (4) GDPR, so that CSIRTs in case of important reasons in relation to that public interest can exchange personal data to CERTs and CSIRTs of third countries. • The GDPR provides clear rules on the transfer of personal data to third countries, within which this proposal is placed and must be understood. This means that the exchange of personal data by CSIRTS in relation to their tasks will only be possible in case of important reasons of public interest, especially in case of a
Rec 69 [GDPR]	The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. …	The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. **The transfer of personal data by CSIRTs to a third country or an international organization, may be necessary for important reasons of public interest, to the extent that this is strictly necessary and proportionate for the purposes of ensuring network and information security by essential or important entities, as referred to in Annex I and II, especially in case of a significant cyber threat or any incident having a significant impact on the provision of services, in the light of the objectives of this Directive and in particular the tasks of CSIRTs for the aforementioned entities.**	

Art. 10 (3a) [GDPR]	New paragraph	**CSIRTs shall establish cooperation relationships with national CERTs and CSIRTs of third countries and may exchange relevant, necessary and proportionate information, in view of the tasks of the CSIRTs, which, in this context, can create an important reason of public interest.**	significant cyber threat of any incident having a significant impact on the provision of services. • Exchange by CSIRTs for the reasons aforementioned would also greatly benefit the important joint work of CSIRTs all over the world to ensure the cybersecurity of our societies and economies. • That is why we propose the formulated new paragraph in article 10, and related to this some additions to the recitals.
21 (1) [CSA]	In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.	~~In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.~~ **a) Member States may provide that essential or important entities can certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 to establish a presumption of conformity with certain requirements of Article 18. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.** **b) Member States may provide that that essential or important entities are required to certify certain ICT products, ICT services and ICT processes under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 to demonstrate conformity with certain**	• It is desirable to add an option for Member States to require OES to certify ICT products, ICT services and ICT processes to demonstrate a presumption of conformity. • It provides the possibility of a more light touch approach where mandatory certification is not (yet) appropriate and gives the opportunity to ascertain whether a certain certification works in practice for important and essential entities.

		requirements of Article 18. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.	
21 (2) [CSA]	The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.	~~The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.~~ **The Commission shall be empowered to adopt implementing acts specifying which categories of essential entities can demonstrate a presumption of conformity or are required to demonstrate conformity with certain requirements of Article 18, by certifying certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential entity or procured from third parties. When preparing the implementing act, the Commission shall:** **(a) take into account the impact of the measures on the manufacturers or providers of such ICT products, ICT services or ICT processes and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, ICT services or ICT processes;** **(b) take into account the existence and implementation of relevant Member State and third country law;**	• More clarity in article 21 (2) could be provided by formulating it separately from 21 (1). • Furthermore, also in this case the option of presumption of conformity would be advantageous, as in 21(1). • Last, due diligence on the consequences of certification should be part of the process, following the example of article 56 (2) of regulation (EU) 2019/881. • Furthermore, we would propose to use the mechanism of implementing acts.

		(c) carry out an open, transparent and inclusive consultation process with all relevant stakeholders and Member States; **(d) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, ICT services or ICT processes, including SMEs;**	
21 (3) [CSA]	The Commission may request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.	The Commission may request ENISA to prepare a candidate scheme **or to review an existing European cybersecurity certification scheme** pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.	• The NIS2 could lead to new requirements that could fit within existing certification schemes. • Adding the option to review existing schemes would help in this situation.